

Notice of Allowability

Application No.

10/071,455

Examiner

Thomas M. Ho

Applicant(s)

BACCHUS ET AL.

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 11/13/06.
2. ☒ The allowed claim(s) is/are 1-13,22,25,26 and 29-50.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.


THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____


KAMBIZ ZAND
PRIMARY EXAMINER

DETAILED ACTION

1. Claims 1-13, 22, 25-26, 29-50 are pending.
2. The RCE of 11/13/06 has been received and entered.

Reasons for Allowance

In reference to claim 1:

“Cryptography and Network Security, Principles and Practice”, Stallings, Chapter 14, “Web Security” discloses a method of providing data from a service to a client over a telecommunication network based on encryption capabilities of the client, the method comprising the computer-implemented steps of:

- At an intermediate server, creating and storing a mapping that associates encryption types to a plurality of available online services, wherein each of the plurality of online services is provided by one or more of a plurality of servers;
- Wherein the intermediate server is coupled to the client and to a plurality of servers ;
- At the intermediate server
- Receiving from the client a request for data and a list of encryption types representing encryption capabilities that are available at the client, where the request from the client is the client hello, and the list of encryption types is the cipher suite which is the list containing the combinations of cryptographic algorithms supported by the client. (pages 451-452)

- Determining an encryption type match by matching the list of encryption types received from the client to the mapping of encryption types to the plurality of online services, where the ciphersuite contains a list of supported encryption algorithms list provided by the client and where the list contains the encryption algorithms that are available or “available online services” (pages 451-453) and the server determines an encryption type match by selecting one of the supported encryption types from the list to use. (page 452, 1st and 2nd paragraph)
- Selecting, from the plurality of online services, an online service that can provide the data to the client based on the encryption type match wherein selecting the online service comprises selecting a particular server from the plurality of servers that provides the online service, where the selection of the service is performed in the server_hello message and a ciphersuite is selected by the server from the list provided by the client. (pages 451-453) & (page 452, 1st and 2nd paragraph)
- Causing communication of the data from the selected online service to the client, where the server_hello message is communicated to the client. (Figure 14.6) & (pages 451-453)

“Cryptography and Network Security, Principles and Practice”, Stallings, Chapter 14, “Web Security” fails to disclose selecting a particular server from the plurality of servers that provides the online service where the selection is based on the encryption type match or mapping.

With regards to this limitation, the Examiner previously rejected the similar limitation of claim 9 as follows:

“Cryptography and Network Security, Principles and Practice”, Stallings, Chapter 14, “Web Security” fails to disclose:

- Selecting a server farm based on the service; and*
- Selecting a particular server in the server farm to provide data to the client.*

The Examiner takes official notice that server farms were well known in the art at the time of invention. For Example, access to large corporate sites, or sites that handle heavy traffic cannot deal with the network and computational load with only a single server. Rather, a large set of servers, all operated by that one entity work together to handle the client load. For Example, google.com does not use a single server to handle all the traffic it encounters from use of its search engine. Rather this work is split among a set of servers associated and commonly owned. Each server within the server farm handles the load through a particular distribution method. Ultimately it is a single server that provides data to a client, although which particular server within the farm may change.

It would have been obvious to one of ordinary skill in the art at the time of invention to select a server farm to deal with the large computational loads required by SSL and especially a large number of clients requiring SSL, while selecting a particular server within the server farm to provide data to the client in order to handle the computational and network burden that a server would not be able to single-handedly provide.

Art Unit: 2132

While it is true that selecting a server farm based on the service and selecting a particular server farm within the farm to provide data to the client is well known in the art, there is no explicit teaching to select a particular server from the plurality of servers where the selection process is based on an encryption mapping or an encryption type match as indicated by Applicant's independent claims.

For Example, suppose the Applicant selected the usage of the GOOGLE_{tm} search engine. It would be evident to one of ordinary skill in the art that GOOGLE corporation handles a large multitude of servers (i.e. a server farm) to provide the search engine service to its users. It is also apparent that at least one of those servers in that multitude will provide the desired service to the client. The selection of the server itself is commonly based on the load or bandwidth requirements of the server/user and remains largely unspecified by the clients actions save for the general type of service desired to be rendered. (Search engine, HTTP, FTP, Realmedia)

In contrast the amended applicants claims calls for the selection of a particular server where the selection is based upon the encryption type match that was formed by matching a list of encryption types received from a client. Thus, Applicant's amendments recite a degree of specificity that is greater than what is readily known in the art. No art had been found which recites this limitation, nor has any explicit motivation been found to modify the invention to yield the recitation of the claims.

For this reason claim 1 is allowable.

Independent claims 11, 13, 22, 25, 26, 49, 50 have all been found to recite the same amended subject matter and primary subject matter as independent claim 1, and are allowable for the same reasons.

Conclusion

3. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on **(571)272-3799**

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist	Telephone: 571-272-2100	Fax: 703-872-9306
Customer Service Representative	Telephone: 571-272-2100	Fax: 703-872-9306

TMH

December 20th, 2006



KAMBIZ ZAND
PRIMARY EXAMINER

Application/Control Number: 10/071,455
Art Unit: 2132

Page 7